

A Parametrized Set of Cyclic Cubic Fields with Even Class-Number

H. J. GODWIN

*Department of Statistics and Computer Science, Royal Holloway College,
Egham Hill, Egham, Surrey TW20 OEX, England*

Communicated by P. Roquette

Received March 14, 1984

It is shown that certain cyclic cubic fields, defined in terms of a parameter, have even class-number. © 1986 Academic Press, Inc.

In the course of an attempt to extend the work of Smith [4] on the Euclidean nature of cyclic cubic fields, it has been found that a certain set of such fields can be shown to have an even class-number.

THEOREM. *Let $B > 1$ be an odd positive integer, and put $4d = 27B^4 + 1$. If the polynomial $x^4 - (9B^2 + 1)x^2 - 8xB^2 + (3B^2 - 1)^2/4$ has no rational zeros then the class-number of the cyclic cubic field with discriminant d^2 defined by*

$$\theta^3 - \theta^2 - \frac{9B^4 - 1}{4}\theta + B^4 = 0 \quad (1)$$

is even.

Proof. The conjugates of θ are

$$\phi = \left(\theta^2 - \frac{B^2 + 1}{2}\theta - \frac{3B^4 - B^2}{2} \right) / B^2$$

and $\psi = 1 - \theta - \phi$.

Since (1) can be written as

$$\left(\theta - \frac{1}{3} \right)^3 - \frac{d}{3} \left(\theta - \frac{4}{9} \right) = 0$$

no factor of d divides the index of θ .

An integral basis for the field is $(1, \theta, \phi)$, and $\varepsilon = (3\phi - 1)/(3\theta - 1) = 6\phi + 3\theta - (9B^2 + 7)/2$ is a unit. ε and either of its conjugates ε_ϕ , ε_ψ form a pair of fundamental units. To show this we note that

$$((\varepsilon - \varepsilon_\phi)^2 + (\varepsilon_\phi - \varepsilon_\psi)^2 + (\varepsilon_\psi - \varepsilon)^2)/2 = 27d$$

and that $((\mu - \mu_\phi)^2 + (\mu_\phi - \mu_\psi)^2 + (\mu_\psi - \mu)^2)/2 = d(q^2 - qr + r^2)$, where $\mu = p + q\theta + r\phi$ is an integer of the field, and $\mu_\phi = p + q\phi + r\psi$, $\mu_\psi = p + q\psi + r\theta$. It follows from Lemma 3 in [1] that $\varepsilon, \varepsilon_\phi$ form a pair of fundamental units if $d^2 > 3^7/2$, i.e., if $B > 1$.

Since $\varepsilon + \varepsilon_\phi + \varepsilon_\psi = 9 - 3(9B^2 + 7)/2 < 0$ it follows that none of $\varepsilon, \varepsilon_\phi, \varepsilon\varepsilon_\phi$ is totally positive. Equation (1) can also be written as

$$\theta \left(\theta - \frac{3B^2 + 1}{2} \right) \left(\theta + \frac{3B^2 - 1}{2} \right) = -B^4, \quad (2)$$

whence B divides the norm of $\lambda = (3B^2 + 1)/2 - \theta$, and since B also divides the norm of $\theta - \phi$, $(B, \lambda, \theta - \phi)$ is a proper ideal, π say. The conjugate of π obtained by replacing θ, ϕ by ψ, θ is $\pi_\psi = (B, \lambda, \phi)$ and we have $\pi\pi_\psi = (B, \lambda, B_\phi)$ and $(\pi\pi_\psi)^2 = (B^2, \lambda, B^2\phi)$.

Since, from (2), $B^2/\lambda = \theta(\theta + (3B^2 - 1)/2)/B^2 = \phi + 2\theta + (3B^2 - 1)/2$ is an integer, it follows that $(\pi\pi_\psi)^2$ is the principal ideal (λ) . λ is totally positive and satisfies

$$\lambda^3 - \left(\frac{9B^2 + 1}{2} \right) \lambda^2 + \frac{9B^2 + 3}{2} B^2 \lambda - B^4 = 0,$$

and if λ is a perfect square then there exist rational integers x, y such that

$$x^2 - 2y = (9B^2 + 1)/2, y^2 \pm 2B^2x = (9B^2 + 3) B^2/2. \quad (3)$$

From (3) we have

$$x^4 - (9B^2 + 1) x^2 \pm 8xB^2 + (3B^2 - 1)^2/4 = 0 \quad (4)$$

and, by considering positive and negative values of x , we may replace the sign \pm by $-$.

But, by the condition of the theorem, (4) gives no solution for x : hence λ is not a perfect square, $\pi\pi_\psi$ is not a principal ideal, and the class-number of the field is even.

REMARKS

1

If d has t distinct prime factors it is known that the class-number of the field is divisible by 3^{t-1} (see [3]). The case of greatest interest is when d is

prime and the theorem then shows that the field is non-Euclidean. If d is prime then there is only one cyclic cubic field with discriminant d^2 , whereas if d is composite there is more than one, but the theorem applies only to the one defined by (1).

2

If $(3B^2 - 1)/2$ is a prime p then the only possible values for x to satisfy (4) are ± 1 , $\pm p$, $\pm p^2$ and, for $B > 1$, it can be verified that none of these do.

3

Calculations show that there are 73 values of B in $[3, 999]$ for which d is prime, and for all of these the condition of the theorem is satisfied. The values of B less than 100 are 3, 5, 19, 23, 25, 37, 47, 49, 51, 73, 77, 79, and 93; the exact class-numbers corresponding to $B=3$ and 5 were given by Gras [2].

REFERENCES

1. H. J. GODWIN, The determination of units in totally real cubic fields, *Proc. Cambridge Philos. Soc.* **56** (1960), 318–321.
2. M. N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbb{Q} , *J. Reine Angew. Math.* **277** (1975), 89–116.
3. H. HEILBRONN, On Euclid's algorithm in cubic self-conjugate fields, *Proc. Cambridge Philos. Soc.* **46** (1950), 377–382.
4. J. R. SMITH, On Euclid's algorithm in some cyclic cubic fields, *J. London Math. Soc.* **44** (1969), 577–582.